Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
European Journal of Combinatorics 26 (2005) 665–682
European Journal of Combinatorics
www.elsevier.com/locate/ejc

Partial permutation decoding for codes from finite planes

J.D. Key[a], T.P. McDonough[b], V.C. Mavron[b]

[a] *Department of Mathematical Sciences, Clemson University, Clemson, SC 29634, USA*
[b] *Department of Mathematics, University of Wales, Aberystwyth, Ceredigion, SY23 3BZ, UK*

Received 17 October 2003; received in revised form 17 April 2004; accepted 22 April 2004
Available online 19 June 2004

Abstract

We determine to what extent permutation decoding can be used for the codes from desarguesian projective and affine planes. We define the notion of s-PD-sets to correct s errors, and construct some specific small sets for $s = 2$ and 3 for desarguesian planes of prime order.

1. Introduction

The codes from finite geometries are the well known generalized Reed–Muller codes, and subfield subcodes of these. They have the projective and affine semi-linear groups as automorphism groups and are good candidates for the use of permutation decoding. Here we examine to what extent permutation decoding can be used for the codes from finite desarguesian planes. We define the notion of partial permutation decoding using sets of automorphisms that can correct up to s errors, where s is some number less than t, the full error-correction capability of the code, calling these s-PD-sets. We obtain explicit s-PD-sets for some of the codes.

The automorphism group of a desarguesian geometry is 2-transitive on points so clearly the whole group will act as a 2-PD-set. Naturally we would like to find smaller 2-PD-sets and also to ask for which s up to the full error-correction capability can we find s-PD-sets. We find partial solutions to these questions in this paper. In particular, we show in Section 3, Propositions 3.2 and 3.3, that 3-PD-sets exist for the codes and their duals for all desarguesian projective planes for any choice of information symbols

E-mail address: vcm@aber.ac.uk (V.C. Mavron).

0195-6698/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ejc.2004.04.007

and that 4-PD-sets exist for particularly chosen information sets. A similar, but weaker, set of results is obtained for affine desarguesian planes. In Section 4 we obtain specific 2-PD-sets for desarguesian planes of prime order for particular known information sets: see Proposition 4.2 which uses an information set from a Singer cycle; Proposition 4.3, using a Moorhouse [16] basis, where we construct 2-PD-sets of 37 elements for desarguesian affine planes of any prime order p; and Proposition 4.4, again using a Moorhouse basis, where we construct 2-PD-sets of 43 elements for desarguesian projective planes of any prime order p. In Proposition 4.5 we obtain 3-PD-sets for the code and the dual code in the affine prime case of sizes $2p^2(p-1)$ and p^2, respectively, and we show that the set for the dual code is minimal. In Section 5 we give a table of some computational results of sizes of s-PD-sets obtained for codes from planes of relatively small order, where we used Magma [3] or GAP [7] for the computations.

Finally in the Appendix, we show that PD-sets for full error-correction for projective desarguesian planes do not exist for order q large enough: Table 2 shows that for $q = p$ prime and $p > 103$, $q = 2^e$ and $e > 12$, $q = 3^e$ and $e > 6$, $q = 5^e$ and $e > 4$, $q = 7^e$ and $e > 3$, $q = 11^e$ and $e > 2$, $q = 13^e$ and $e > 2$, or $q = p^e$ for $p > 13$ and $e > 1$, PD-sets for full error-correction cannot exist, with similar results holding for the affine and dual cases. This is in contrast to some binary codes obtained from graphs with the symmetric group acting, where PD-sets were found for the infinite class of codes: see [11, 12].

2. Background

Following generally the notation in [1], an incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a t-(v, k, λ) design, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks. The design is **symmetric** if it has the same number of points and blocks.

If F is the field $\mathbb{F}_p$ of order p where p is a prime, the **code** $C_F(\mathcal{D})$ (or $C_p(\mathcal{D})$) of the design $\mathcal{D}$ over F is the space spanned by the incidence vectors of the blocks over F. If the point set of $\mathcal{D}$ is denoted by $\mathcal{P}$ and the block set by $\mathcal{B}$, and if $\mathcal{Q}$ is any subset of $\mathcal{P}$, then we will denote the incidence vector of $\mathcal{Q}$ by $v^{\mathcal{Q}}$. Thus $C_F(\mathcal{D}) = \langle v^B | B \in \mathcal{B} \rangle$, and is a subspace of $F^{\mathcal{P}}$, the full vector space of functions from $\mathcal{P}$ to F. The dimension of $C_p(\mathcal{D})$ is called the p-rank of $\mathcal{D}$.

The codes here will be **linear codes**, i.e. subspaces of the ambient vector space. If a code C over a field of order q is of length n, dimension k, and minimum weight d, then we write $[n, k, d]_q$ to show this information. A **generator matrix** for the code is a $k \times n$ matrix made up of a basis for C. The **dual** or **orthogonal** code $C^\perp$ is the orthogonal subspace under the standard inner product $(,)$, i.e. $C^\perp = \{v \in F^n \mid (v, c) = 0 \text{ for all } c \in C\}$. A **check** (or **parity-check**) matrix for C is a generator matrix H for $C^\perp$; the **syndrome** of a vector $y \in F^n$ is Hy^T. A code C is **self-orthogonal** if $C \subseteq C^\perp$ and is **self-dual** if $C = C^\perp$. If $c \in C$ then the **support** of c is the set of non-zero coordinate positions of c, and the **weight** of c is the cardinality of the support. A **constant vector** is one for which all the non-zero coordinate entries are the same. The **all-one vector** will be denoted by $\boldsymbol{\jmath}$, and is the constant vector of weight the length of the code. Two linear codes of the same

length and over the same field are **isomorphic** if they can be obtained from one another by permuting the coordinate positions. Any code is isomorphic to a code with generator matrix in so-called **standard form**, i.e. the form $[I_k \mid A]$; a check matrix then is given by $[-A^T \mid I_{n-k}]$. The first k coordinates are the **information symbols** (or set) and denoted by $\mathcal{I}$, and the last $n-k$ coordinates are the **check symbols**, denoted by $\mathcal{C}$. An **automorphism** of a code C is an isomorphism from C to C. The automorphism group will be denoted by $\mathrm{Aut}(C)$. Any automorphism clearly preserves each **weight class** of C, i.e. the set of vectors of C of a given weight.

For any finite field $\mathbb{F}_q$ of order q, the set of points and r-dimensional subspaces (respectively flats) of an m-dimensional projective (respectively affine) geometry forms a 2-design which we will denote by $\mathrm{PG}_{m,r}(\mathbb{F}_q)$ (respectively $\mathrm{AG}_{m,r}(\mathbb{F}_q)$). In particular, the **desarguesian projective** and **affine planes** of order q are denoted by $\mathrm{PG}_{2,1}(\mathbb{F}_q)$ (respectively $\mathrm{AG}_{2,1}(\mathbb{F}_q)$) but we will simply use $\mathrm{PG}_2(\mathbb{F}_q)$ and $\mathrm{AG}_2(\mathbb{F}_q)$, as is customary. The **automorphism groups**, $P\Gamma L_{m+1}(\mathbb{F}_q)$ or $A\Gamma L_m(\mathbb{F}_q)$, respectively, of these designs (and codes) are the full projective or affine semi-linear groups, and always 2-transitive on points. If $q = p^e$ where p is a prime, the codes of these designs are over $\mathbb{F}_p$ and are subfield subcodes of the generalized Reed–Muller codes: see [1, Chapter 5] for a full treatment. The dimension and minimum weight is known in each case: see [1, Theorem 5.7.9]. In particular, in the case of planes, which is what we consider here, the result is as follows:

Result 2.1. If $q = p^e$, the p-rank of the design of points and lines of $\mathrm{PG}_2(\mathbb{F}q)$ is $\binom{p+1}{2}^e + 1$ and that of the design of points and lines of $\mathrm{AG}_2(\mathbb{F}_q)$ is $\binom{p+1}{2}^e$. In both cases the minimum weight vectors are the incidence vectors of the lines and their scalar multiples.

The dual codes of the codes from the finite geometry designs are not, in general, generalized Reed–Muller codes, and much less is known about their minimum weights except in the case $p = 2$, or in the prime case. For desarguesian planes of order $q = p^e$ where p is prime, the minimum weight $d^\perp$ of $C^\perp$ satisfies

$$q + p \le d^\perp \le 2q, \tag{1}$$

with equality at the lower bound for $p = 2$, and at $q = p$. See [4–6] for improvements on this in the case of p odd.

Permutation decoding was first developed by MacWilliams [14] and involves finding a set of automorphisms of a code called a PD-set. The method is described fully in MacWilliams and Sloane [15, Chapter 15] and Huffman [9, Section 8]. We extend the definition of PD-sets to s-PD-sets for s-error-correction:

Definition 2.2. If C is a t-error-correcting code with information set $\mathcal{I}$ and check set $\mathcal{C}$, then a **PD-set** for C is a set $\mathcal{S}$ of automorphisms of C which is such that every t-set of coordinate positions is moved by at least one member of $\mathcal{S}$ into the check positions $\mathcal{C}$.

For $s \le t$ an s-**PD-set** is a set $\mathcal{S}$ of automorphisms of C which is such that every s-set of coordinate positions is moved by at least one member of $\mathcal{S}$ into $\mathcal{C}$.

That a PD-set will fully use the error-correction potential of the code follows easily and is proved in Huffman [9, Theorem 8.1]. That an s-PD-set will correct s errors also

follows, and we restate this result in order to use our s-PD-sets for s-error-correction, where $s \leq t$:

Result 2.3. Let C be an $[n, k, d]_q$ t-error-correcting code. Suppose H is a check matrix for C in standard form, i.e. such that I_{n-k} is in the redundancy positions. Let $y = c + e$ be a vector, where $c \in C$ and e has weight $s \leq t$. Then the information symbols in y are correct if and only if the weight of the syndrome Hy^T of y is $\leq s$.

The algorithm for permutation decoding is as follows: we have a t-error-correcting $[n, k, d]_q$ code C with check matrix H in standard form. Thus the generator matrix $G = [I_k \mid A]$ and $H = [-A^T \mid I_{n-k}]$, for some A, and the first k coordinate positions correspond to the information symbols. Any vector v of length k is encoded as vG. Suppose x is sent and y is received and at most s errors occur, where $s \leq t$. Let $\mathcal{S} = \{g_1, \ldots, g_m\}$ be an s-PD-set. Compute the syndromes $H(yg_i)^T$ for $i = 1, \ldots, m$ until an i is found such that the weight of this vector is s or less. Compute the codeword c that has the same information symbols as yg_i and decode y as cg_i^{-1}.

Such sets might not exist at all, and the property of having a PD-set might not be invariant under isomorphism of codes, i.e. it depends on the choice of $\mathcal{I}$ and $\mathcal{C}$. Furthermore, there is a bound on the minimum size that the set $\mathcal{S}$ may have, due to Gordon [8], from a formula due to Schönheim [17], and quoted and proved in [9]:

Result 2.4. If $\mathcal{S}$ is a PD-set for a t-error-correcting $[n, k, d]_q$ code C, and $r = n - k$, then

$$|\mathcal{S}| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil.$$

This result can be adapted to s-PD-sets for $s \leq t$ by replacing t by s in the formula.

To obtain PD-sets, one needs a generator matrix for the code in standard form, and thus one needs to know what to take as information symbols. Even for desarguesian planes, general sets of information symbols are not known; in the projective case the fact that the code is cyclic can be used, and, in the case of planes of prime order, we have the following result of Moorhouse [16]:

Result 2.5 (Moorhouse). Let $\pi = \mathrm{AG}_2(\mathbb{F}_p)$ where p is a prime. A basis for the code $C_p(\pi)$ can be found by taking the incidence vectors of the following lines: all the p lines from any one parallel class; any $p - 1$ lines from any other parallel class; and so on, until a single line is chosen from one of the final two parallel classes, and no lines are chosen from the remaining class. This gives

$$p + (p-1) + (p-2) + \cdots + 1 = p(p+1)/2 = \binom{p+1}{2}$$

lines, whose incidence vectors form a basis for $C_p(\pi)$.

Similarly, a basis for the desarguesian projective plane of prime order can be found by including the line at infinity. By using homogeneous coordinates for the projective case, one sees that a basis for the plane will show how to find an information set.

Another basis for the prime case was given by Blokhuis and Moorhouse [2]:

Result 2.6. Let $\Pi = \mathrm{PG}_2(\mathbb{F}_p)$ where p is a prime, and let $\mathcal{C}$ denote a conic in Π. Then a basis for the code $C_p(\Pi)$ can be found by taking the incidence vectors of all nonsecants to $\mathcal{C}$, i.e. all tangents and exterior lines.

A basis for $C_p(\Pi)^\perp$ can be found by taking the complements of the incidence vectors of the secants.

3. Existence of *s*-PD-sets for desarguesian planes

We show that both the code and its dual of any desarguesian projective plane will have 3-PD-sets no matter what information set $\mathcal{I}$ is chosen. To ensure that the code will correct three errors, we will take the order $q \geq 7$; for the dual code, where the minimum weight in the case $q = p$ prime is $2p$, we need $q \geq 5$. In general our bounds on the order relate to the error-correction capability of the code, which might not be the same as that of its dual. First we need a lemma.

Lemma 3.1. *If $q = p^e \geq 5$, where p is a prime, then*

1. $(p(p+1)/2)^e > p^e + 2$ *and* $p^{2e} - (p(p+1)/2)^e > p^e + 2$;
2. $(p(p+1)/2)^e + 1 > p^e + 2$ *and* $p^{2e} + p^e + 1 - (p(p+1)/2)^e - 1 > p^e + 2$.

Proof. The proof of this is quite direct, so we omit it. □

We use these inequalities to prove the existence of 3-PD-sets for desarguesian planes:

Proposition 3.2. *Let $\Pi = \mathrm{PG}_2(\mathbb{F}_q)$, where $q = p^e$ and p is a prime, $C = [q^2 + q + 1, (p(p+1)/2)^e + 1, q+1]_p$ its p-ary code, and G its automorphism group. Then if $q \geq 7$, a 3-PD-set can be found in G for C using any information set; similarly for $q \geq 5$ for the dual code $C^\perp = [q^2 + q + 1, q^2 + q - (p(p+1)/2)^e, d^\perp]_p$ where $q + p \leq d^\perp \leq 2q$.*

If $q \geq 8$, information sets exist for C such that 4-PD-sets can be found in G; similarly for $C^\perp$ for $q \geq 5$.

Proof. Note first that G is transitive on triangles and on collinear triples of points: see, for example, [10, Chapter 2].

Concerning 3-PD-sets, let $\mathcal{I}$ denote information symbols for C and $\mathcal{C}$ the check symbols, and let $\mathcal{T} = \{P_1, P_2, P_3\}$ be a set of three points. We first show that both $\mathcal{I}$ and $\mathcal{C}$ contain both triangles and sets of collinear triples. In fact, if a set of points in Π has no three points collinear, then it must be an arc in the plane and hence of size at most $q + 2$. Both $\mathcal{I}$ and $\mathcal{C}$ have size bigger than this by Lemma 3.1, so this is impossible. Also, neither $\mathcal{I}$ nor $\mathcal{C}$ can have all points collinear since this would restrict their size to $q + 1$. Thus both types of triple occur in both $\mathcal{I}$ and $\mathcal{C}$. By transitivity then, $\mathcal{T}$ can be mapped to the error positions by some member of G, in the case of C and in the case of $C^\perp$.

For 4-PD-sets, we need to consider sets of four points in Π. Such a set is either a quadrangle, or a point and three collinear points, or all four collinear points. Again taking $\mathcal{I}$ for the information symbols and $\mathcal{C}$ for the check symbols, using the lemma we see that both $\mathcal{I}$ and $\mathcal{C}$ contain 4-sets of the first two types. Since G is transitive on these types of 4-set, we can always map such a 4-set to the check symbols. In the case of sets of four collinear points, we do not have transitivity. We have to ensure that $\mathcal{C}$ (for C) and $\mathcal{I}$

(for $C^\perp$) contains a representative of every orbit of G acting on collinear 4-sets. Since G is transitive on incident point–line pairs and since $q \geq 4$, each line excluding an arbitrary point contains such representatives.

We may choose $\mathcal{I}$ for C by starting with an information set for a corresponding affine plane and adding a point from the line at infinity. In this case $\mathcal{C}$ will contain a line excluding one point. Thus, $\mathcal{C}$ has a 4-PD-set in this case.

Now let L be any line of $\mathrm{PG}_2(\mathbb{F}_q)$, let $P_1, \ldots, P_{q+1}$ be the points of L, let P be a point off L and let L_i be the line joining P to P_i, $i = 1, \ldots, q+1$. Then $v^{L_1}, \ldots, v^{L_{q+1}}$ are independent and yield I_{q+1} when restricted to the positions $P_1, \ldots, P_{q+1}$. Hence, we may choose $\mathcal{I}$ to contain $P_1, \ldots, P_{q+1}$. With the corresponding check set as the information set, $C^\perp$ has a 4-PD-set. □

Similar results hold for the desarguesian affine planes, but we have to be more restrictive in our choice of information set since we do not have transitivity on collinear triples of points:

Proposition 3.3. *Let $\pi = \mathrm{AG}_2(\mathbb{F}_q)$ where $q = p^e$ and p is a prime, $C = [q^2, (p(p+1)/2)^e, q]_p$ its p-ary code, and G its automorphism group. Then if $q \geq 7$, a 3-PD-set can be found in G for C. Similarly, for $q \geq 5$, a 3-PD-set can be found in G for the dual code $C^\perp = [q^2, q^2 - (p(p+1)/2)^e, d^\perp]_p$ where $q + p \leq d^\perp \leq 2q$.*

Proof. As in the projective case, but using the alternative inequalities in Lemma 3.1, we see that all possible information sets and check sets contain triangles and collinear triples.

We may choose $\mathcal{I}$, as in the last paragraph of the proof of Proposition 3.2, to contain the points of an (affine) line. With the corresponding check set as information set, $C^\perp$ has a 4-PD-set, since every G-orbit of collinear triples has a triple on this line.

To show that $\mathcal{C}$ may be chosen to contain a line excluding a point, we work with the column vectors of the incidence matrix of the affine plane mod p. Let u_P denote the column vector corresponding to the point P. Choose a line L and a point P on it. Let Q be any other point of L. Let $A \neq L$ be a line on P and let B be the line on Q parallel to A. It is easy to see that $\sum_{R \in B} u_R = \sum_{R \in A} u_R$. Hence, u_Q is a linear combination of u_P and the vectors u_R, $R \notin L$. So, an information set can be selected from $\{R : R \notin L\} \cup \{P\}$. The corresponding check set contains $\{Q : Q \in L, Q \neq P\}$. Consequently, C has a 3-PD-set. □

Note. For $q = p$ using the Moorhouse [16] basis of Result 2.5, both the information and check sets will contain either a line or a line excluding one point. We can now use this basis to obtain a similar result for prime-order affine planes for 4-PD-sets; the basis we use is discussed fully in Section 4.

Proposition 3.4. *Let $\pi = \mathrm{AG}_2(\mathbb{F}_p)$ where p is a prime and $p \geq 11$, $C = \left[p^2, \binom{p+1}{2}, p\right]_p$ its p-ary code, and G be its automorphism group. Then G contains a 4-PD-set for the code using information set*

$$\mathcal{I} = \{(i, j) \mid 0 \leq i \leq j \leq p-1\},$$

and check set

$$\mathcal{C} = \{(i, j) \mid p - 1 \geq i > j \geq 0\}.$$

The same result is true for $p \geq 5$ *for* $C^{\perp} = \left[p^2, p^2 - \binom{p+1}{2}, 2p\right]_p$ *(using* $\mathcal{C}$ *as information set).*

Proof. For the result to be true for C, the check positions must contain a representative of every orbit of 4-sets of points. In the affine case there are more orbits and more geometrical configurations than in the projective case, and G is transitive on triangles but not on quadrangles. The basic types of configuration are the same as in the projective case: four points collinear, exactly three collinear, or a quadrangle. Although G is transitive on triangles, it is not transitive on collinear triples and thus the first two types of 4-set are in more than two orbits. However, if we ensure that $\mathcal{C}$ has at least $p - 1$ collinear points, then these two configurations are taken care of. Clearly $\{(i, 0) \mid 1 \leq i \leq p - 1\}$ is such a set. For the quadrangles, since G is transitive on triangles, we need only show that the quadrangle $\{(0, 0), (1, 0), (0, 1), (a, b)\}$ (where $a \neq 0, b \neq 0, a + b \neq 1$) can be mapped into a quadrangle of points in $\mathcal{C}$. This can easily be shown to be possible using a suitable translation $\tau_{i,j} : (x, y) \mapsto (x, y) + (i, j)$, where $p - 2 \geq i \geq j + 2 \geq 2$ (working (mod p)). This shows that every 4-set can be mapped to $\mathcal{C}$ and that G will thus contain a 4-PD-set for C.

The result for $C^{\perp}$ follows similarly. □

4. Explicit 2-PD sets for planes of prime order

Now we consider planes of prime order p. We give explicit 2-PD-sets for codes of these planes for two distinct sets of information symbols.

First we have a general result for cyclic codes of a particular dimension. Note that by the standard definition of a cyclic code of dimension k and length n with co-ordinate positions $0, 1, \ldots, n-1$, the n-cycle $(0, 1, \ldots, n-1)$ is in the automorphism group of the code and thus any k consecutive positions can be taken as the information symbols. Note also that throughout we will write our maps on the right and, correspondingly, use row vectors for points of the geometrical designs and write our matrices on the right.

Proposition 4.1. *Let* $C = [n, k, d]_q$ *be a cyclic code of odd length* n *over the field* $\mathbb{F}_q$ *of order* q*, where* $k = (n + 1)/2$*,* $(n, q) = 1$ *and* $d \geq 5$*. Label the coordinate positions* $0, 1, \ldots, n - 1$ *and take* $\mathcal{I} = \{0, 1, \ldots, k - 1\}$ *for the information symbols. Let* $A = \mathrm{Aut}(C) \leq S_n$*, and let* $\sigma : i \mapsto i + 1$ *and* $\mu : i \mapsto qi \pmod{n}$*. If* $S = \langle \sigma \rangle$ *and* $q \not\equiv \pm 1 \pmod{n}$*, then* $\mathcal{S} = S \cup \mu S$ *is a 2-PD-set of size* $2n$ *for* C*.*

Proof. Suppose two errors occur at positions i_1 and i_2, where $0 \leq i_1 < i_2 \leq n - 1$. If either $i_2 - i_1 - 1$ or $(n - 1) - (i_2 - i_1)$ is less than $(n - 3)/2$, then $\{i_1, i_2\}$ can be brought into the check positions by some power of σ.

If $i_1 = 0$ and $i_2 = k = (n + 1)/2$, then $\{0, k\}$ cannot move into the check positions by S. Since $0\mu = 0$ and $k\mu = qk$, if $qk \neq k$ or $k - 1$ then μS will take any pair of positions

to the check positions. This is equivalent to $q \not\equiv \pm 1 \pmod{n}$. Thus $S \cup \mu S$ will form a 2-PD-set provided that $q \not\equiv \pm 1 \pmod{n}$. □

Note. That $\mu \in \mathrm{Aut}(C)$ is proved in MacWilliams [14].

Thus if we take our information positions to be consecutive positions defined by a cycle acting on the code, we will have the following:

Proposition 4.2. *Let $\Pi = \mathrm{PG}_2(\mathbb{F}_p)$ where $p \geq 5$ is a prime, and C the p-ary code of Π. Writing $n = p^2 + p + 1$, then $C = [n, (n+1)/2, p+1]_p$. Let S be the cyclic group generated by a Singer cycle and take $\mathcal{I} = \{0, 1, \ldots, ((n+1)/2) - 1\}$ for the information symbols, as defined by S. Then, in the notation of Proposition 4.1 for σ and μ, $S \cup \mu S$ will form a 2-PD-set for C and S will form a 2-PD-set for $C^\perp$ for $p \geq 3$. Furthermore, the order of μ is 3.*

Proof. It is clear that $p \not\equiv \pm 1 \pmod{n}$, so the proposition gives the first part immediately. Since the dimension of $C^\perp$ is $(n-1)/2 < n/2$, it is immediate (see [14]) that S will suffice for two errors for $C^\perp$.

That μ has order 3 follows since $i(\mu)^3 = p^3 i = i$, because $p^3 \equiv 1 \pmod{p^2 + p + 1}$. □

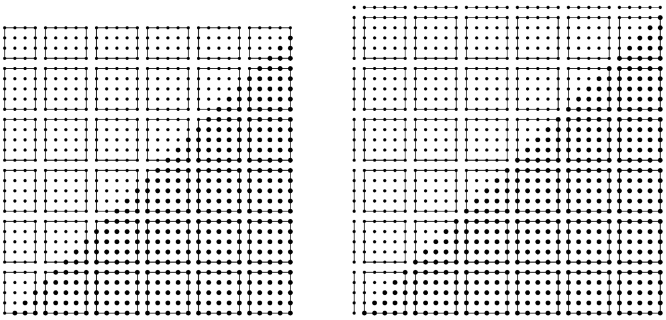
The Moorhouse basis of Result 2.5 extends to a basis for a projective plane of prime order in the natural way by including the incidence vector of the line at infinity. In the projective case, if homogeneous coordinates are used, then it is clear that if we have the homogeneous coordinates for a set of lines that produce a basis for the code of the plane then the points with the same homogeneous coordinates as these lines will form an information set for the code. We can find an information set for the code of the affine desarguesian plane of order p by selecting a projective line which meets an information set of the code of the projective desarguesian plane of order p in a single point and taking this line to be the line at infinity.

In this way it is not difficult to verify that the following points can be taken as information symbols for the p-ary code of the desarguesian affine plane $\mathrm{AG}_2(\mathbb{F}_p)$ of prime order p:

$$\begin{array}{ccccccc} (0,0) & (0,1) & (0,2) & \cdots & & (0,p-1) \\ & (1,1) & (1,2) & \cdots & & (1,p-1) \\ & & (2,2) & \cdots & & (2,p-1) \\ & & & \vdots & & \\ & & & & (p-1,p-1) \end{array} . \tag{2}$$

Here, if we take for the line at infinity $\ell^\infty = (0,0,1)'$, then we take p lines $(1,0,a)'$ for $0 \leq a \leq p-1$ through $(0,1,0)$, $p-1$ lines $(1,1,a)'$ for $1 \leq a \leq p-1$ through $(1,-1,0)$, $p-2$ lines $(1,2,a)'$ for $2 \leq a \leq p-1$ through $(1,-2^{-1},0), \ldots,$ 1 line $(1,p-1,a)'$ for $a = p-1$ through $(1,1,0)$, and then take the corresponding points for our information set, as shown above. Thus the information symbols are

$$\mathcal{I} = \{(i,j) \mid 0 \leq i \leq j \leq p-1\}, \tag{3}$$



A: $p = 29$. B: $p = 31$.

Fig. 1. Affine planes displaying the 'Moorhouse' check set and subdivisions in Proposition 4.3.

and the check symbols

$$\mathcal{C} = \{(i, j) \mid p - 1 \geq i > j \geq 0\}. \tag{4}$$

We will use the following notation for a translation in the affine group $\mathrm{AGL}_2(\mathbb{F}_q)$:

$$\tau_{a,b} : (x, y) \mapsto (x, y) + (a, b), \tag{5}$$

for $(x, y), (a, b) \in \mathrm{AG}_2(\mathbb{F}_q)$.

Proposition 4.3. *Let $\pi = \mathrm{AG}_2(\mathbb{F}_p)$ where $p \geq 5$ is a prime, and C its p-ary code. Let $n = \lfloor (p+1)/6 \rfloor$, and $Y = \{\tau_{un,-vn} \mid 0 \leq u, v \leq 5\}$. Then, using $\mathcal{I} = \{(i, j) \mid 0 \leq i \leq j \leq p - 1\}$ as information set, Y is a 2-PD-set for C if $p \equiv -1 \pmod 6$, and $Y \cup \{\tau_{1,1}\}$ is a 2-PD-set for C if $p \equiv 1 \pmod 6$, i.e. C has a 2-PD-set of size ≤ 37. Furthermore, $(Y \cup \{\tau_{1,1}\})\delta$ is a 2-PD-set of 37 elements for $C^{\perp}$, using $\mathcal{C}$ of Eq. (4) as information set, and where δ is defined in Eq. (10).*

Proof. Clearly $p = 6n \pm 1$. The set $\mathcal{C} = \{(i, j) \mid 0 \leq j < i \leq p - 1\}$ is the check set corresponding to the information set $\mathcal{I}$, and we set $\mathcal{P} = \mathcal{I} \cup \mathcal{C}$. For each u, v with $0 \leq u, v \leq 5$, let $\mathcal{C}_{u,v} = \mathcal{C}\tau_{-un,vn}$.

We now define a partition of $\mathcal{P}$. The partition is illustrated in Fig. 1, A and B, for the primes 29 and 31, respectively.

For $0 \leq u, v \leq 5$, let $S_{u,v} = \{(i, j) \mid \max(0, p - (u + 1)n) \leq i < p - un, vn \leq j < \min((v + 1)n, p)\}$. Clearly, $S_{u,v} \subseteq S_{0,0}\tau_{-un,vn}$ for all u, v $(0 \leq u, v \leq 5)$, with equality unless $p \equiv -1 \pmod 6$ and either $u = 5$ or $v = 5$. We refer to these subsets as 'squares', even though this is slightly inaccurate if $p \equiv -1 \pmod 6$. In this case, the squares partition $\mathcal{P}$.

If $p \equiv 1 \pmod 6$, we define the 'vertical lines' $V_u = \{(0, j) \mid un \leq j < (u + 1)n\}$ and the 'horizontal lines' $H_u = \{(i, p - 1) \mid p - (u + 1)n \leq i < p - un\}$ for $0 \leq u \leq 5$. We refer to $(0, p - 1)$ as the 'top point'. It is easily seen that, when $p \equiv 1 \pmod 6$, $\mathcal{P}$ is partitioned by the squares, the horizontal and vertical lines and the top point.

Let $X = \{\tau_{-un,vn} \mid 0 \leq u, v \leq 5\}$. We will show that $Y = \{\tau^{-1} \mid \tau \in X\}$ is a 2-PD-set for C if $p \equiv -1 \pmod 6$ and $Y \cup \{\tau_{1,1}\}$ is a 2-PD-set for C if $p \equiv 1 \pmod 6$.

We consider first the case $p \equiv -1 \pmod 6$. Let $A = \{(a,b) \mid 0 \le a,b \le 3, a+b \le 3\}$. Then $\mathcal{C}_{u,v}$ contains every square of the form $S_{u+a,v+b}$ with $(a,b) \in A$, reducing subscripts modulo 6. Thus, $S_{u,v}$ is contained in $\mathcal{C}_{u-a,v-b}$ if $(a,b) \in A$. Hence, $S_{u,v}$ and $S_{u-a+c,v-b+d}$ are contained in $\mathcal{C}\tau$ for some $\tau \in X$ if $(a,b),(c,d) \in A$. Computing the differences $(c,d)-(a,b)$ in $\mathbb{Z}_6^2$ for all $(a,b),(c,d) \in A$, we see that the only pairs of squares unaccounted for are those of the form $S_{u,v}$ and $S_{u+2,v+2}$.

To deal with such pairs, we notice that if $2 \le u \le 5$ then $\mathcal{C}_{u,v}$ contains $S_{u+4,v}$, if $2 \le v \le 5$ then $\mathcal{C}_{u,v}$ contains $S_{u,v+4}$, and if either u or v is in $\{4,5\}$ then $\mathcal{C}_{u,v}$ contains $S_{u+2,v+2}$.

Consider the pair $S_{u,v}$ and $S_{u+2,v+2}$ and let u' and v' be chosen so that $0 \le u', v' \le 5$, $u' = u+2$ and $v' = v+2$. If $u < u'$ and $v < v'$ then both squares are in $\mathcal{C}_{u,v'}$, since $v' \ge 2$ and hence $\mathcal{C}_{u,v'}$ contains both $S_{u+2,v'+0}$ and $S_{u+0,v'+4}$. Similarly, if $u < u'$ and $v' < v$ then both squares are in $\mathcal{C}_{u',v}$, if $u' < u$ and $v < v'$ then both squares are in $\mathcal{C}_{u,v'}$, and if $u' < u$ and $v' < v$ then both squares are in $\mathcal{C}_{u',v'}$.

Since we have now shown that every pair from $\mathcal{P}$ is contained in $\mathcal{C}\tau$, for some $\tau \in X$, it follows that Y is a 2-PD-set for C if $p \equiv -1 \pmod 6$.

We now turn to the case $p \equiv 1 \pmod 6$. Let $B = A \cup \{(4,0),(0,4)\}$. Then $\mathcal{C}_{u,v}$ contains every square of the form $S_{u+a,v+b}$ with $(a,b) \in B$, reducing subscripts modulo 6. Arguing as above, we see that pairs of squares of the form $S_{u,v}$ and $S_{u-a+c,v-b+d}$ are contained in $\mathcal{C}\tau$ for some $\tau \in X$ if $(a,b),(c,d) \in B$. Computing the differences $(c,d)-(a,b)$ in $\mathbb{Z}_6^2$ for all $(a,b),(c,d) \in B$, we find that every pair of squares is contained in some $\mathcal{C}\tau$ for some $\tau \in X$.

Next, we observe that the vertical line V_u is contained in $\mathcal{C}_{a+2,u+b+3}$ for all $(a,b) \in E$, where $E = D \cup \{(5,3)\}$ and $D = \{(a,b) \mid 0 \le a,b \le 3, a+b \ge 3\}$. Thus, V_u and $S_{a+2+c,u+b+3+d}$ are contained in $\mathcal{C}\tau$ for some $\tau \in X$ if $(a,b) \in E$ and $(c,d) \in B$. Computing the sums $(a,b)+(c,d)$ in $\mathbb{Z}_6^2$ for all $(a,b) \in E$ and $(c,d) \in B$, we find that every pair consisting of a square and vertical line is contained in some $\mathcal{C}\tau$ for some $\tau \in X$.

A similar argument applies to pairs consisting of a square and horizontal line.

The top point is contained in $\mathcal{C}_{a+2,b+2}$ for every $(a,b) \in D$. Thus, the top point and $S_{a+2+c,b+2+d}$ are contained in $\mathcal{C}\tau$ for some $\tau \in X$ if $(a,b) \in D$ and $(c,d) \in B$. Computing the sums $(a,b)+(c,d)$ in $\mathbb{Z}_6^2$ for all $(a,b) \in D$ and $(c,d) \in B$, we find that every pair consisting of a square and the top point is contained in some $\mathcal{C}\tau$ for some $\tau \in X$, except for the square $S_{1,1}$. However, it is easily seen that the top point and $S_{1,1}$ are contained in $\mathcal{C}\tau_{-1,-1}$.

Let $0 \le v < v' \le 5$. Either $\mathcal{C}_{5,v}$ or $\mathcal{C}_{5,v'}$ will contain both V_v and $V_{v'}$. Also, either $\mathcal{C}_{5,v}$ or $\mathcal{C}_{5,5}$ will contain both V_v and the top point.

Similar arguments apply to the horizontal lines and the top point.

Finally, consider the two lines V_v and H_u where $0 \le u,v \le 5$. The vertical line V_v is contained in $\mathcal{C}_{a+2,v+b+3}$ for all $(a,b) \in E$ and the horizontal line H_u is contained in $\mathcal{C}_{u+c+3,d+2}$ for all $(c,d) \in F$, where $F = D \cup \{(3,5)\}$. Computing the differences $(a,b)-(c,d)$ in $\mathbb{Z}_6^2$ for all $(a,b) \in E$ and $(c,d) \in F$, we find that every pair consisting of a horizontal line and vertical line is contained in some $\mathcal{C}\tau$ for some $\tau \in X$.

This completes the argument that $Y \cup \{\tau_{1,1}\}$ is a 2-PD-set for C if $p \equiv 1 \pmod 6$.

That $(Y \cup \{\tau_{1,1}\})\delta$ is a 2-PD-set for $C^\perp$ in all cases now follows immediately, since the mapping δ interchanges the first and second coordinate. □

We now obtain an analogue for the desarguesian projective planes of prime order. First we define $\mathcal{A} = \{(1, i, j) \mid 0 \le i, j \le p-1\}$, $\mathcal{A}_1 = \{(1, i, j) \mid 0 \le i \le j \le p-1\}$, $\mathcal{L} = \{(0, 1, i) \mid 0 \le i \le p-1\}$ and $P = (0, 0, 1)$ explicitly, and set $\mathcal{A}_2 = \mathcal{A} - \mathcal{A}_1$. Then we can take for an information set $\mathcal{I}_\Pi$ for $C_p(\mathrm{PG}_2(\mathbb{F}_p))$ the set

$$\mathcal{I}_\Pi = \{(1, i, j) \mid 0 \le i \le j \le p-1\} \cup \{(0, 0, 1)\} = \mathcal{A}_1 \cup \{P\}, \tag{6}$$

and the corresponding check set will then be

$$\mathcal{C}_\Pi = \{(1, i, j) \mid p-1 \ge i > j \ge 0\} \cup \{(0, 1, i) \mid 0 \le i \le p-1\} = \mathcal{A}_2 \cup \mathcal{L}. \tag{7}$$

We write the element of $\mathrm{PGL}_3(\mathbb{F}_q)$ corresponding to the translation $\tau_{a,b}$ as

$$\hat{\tau}_{a,b} = \begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}. \tag{8}$$

Proposition 4.4. *Let $\Pi = \mathrm{PG}_2(\mathbb{F}_p)$ where $p \ge 5$ is a prime, and let C be its p-ary code. If $n = \lfloor (p+1)/6 \rfloor$, let*

$$\hat{Y} = \{\hat{\tau}_{un,-vn} \mid 0 \le u, v \le 5\},$$
$$\hat{Y}_0 = \{\hat{\tau}_{0,0}, \hat{\tau}_{0,-(p-\varepsilon)/2}, \hat{\tau}_{-(p+\varepsilon)/2,-(p-\varepsilon)/2}, \hat{\tau}_{-(p-\varepsilon)/2,-p+\varepsilon}\},$$

where $\varepsilon \in \{-1, 1\}$ and $p \equiv \varepsilon \pmod 6$, and

$$\sigma_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad \sigma_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad \sigma_2 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$
$$\sigma_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \quad \sigma_4 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

Then, using the information set $\mathcal{I}_\Pi$ of Eq. (6), C has a 2-PD-set $\hat{Y} \cup \hat{Y}_0 \cup \sigma_0\hat{Y}_0 \cup \{\sigma_1\}$ in the case $p \equiv -1 \pmod 6$ and $\hat{Y} \cup \hat{Y}_0 \cup \sigma_0\hat{Y}_0 \cup \{\sigma_1, \hat{\tau}_{1,1}\}$ in the case $p \equiv 1 \pmod 6$, of size 42 and 43, respectively.

Furthermore, using the information set $\mathcal{C}_\Pi$ of Eq. (7), the set

$$(\hat{Y} \cup \{\hat{\tau}_{1,1}\})\sigma_0 \cup \{\iota, \sigma_2, \sigma_3, \hat{\tau}_{1,1}\sigma_3, \hat{\tau}_{1,1}\sigma_4, \hat{\tau}_{-1,1}\sigma_4, \sigma_4, \sigma_4\sigma_3, \hat{\tau}_{1,0}\sigma_4\}$$

(where ι is the identity map) of size 46 is a 2-PD-set for $C^\perp$.

Proof. Let $\mathcal{C}_\Pi$ be the check set corresponding to $\mathcal{I}_\Pi$. Note that the intersection of $\mathcal{I}_\Pi$ with the point set $\{(1, i, j) \mid 0 \le i, j \le p-1\}$, which is the point set of the affine plane $\mathrm{AG}_2(\mathbb{F}_p)$ obtained by removing the line $\{(0, 1, i) \mid 0 \le i \le p-1\} \cup \{(0, 0, 1)\}$, corresponds to the information set in Proposition 4.3. The translation $\tau_{a,b}$ for that affine plane corresponds to the collineation $\hat{\tau}_{a,b}$ of Π, as given in Eq. (8). Let $\hat{Y} = \{\hat{\tau}^{-1} \mid \tau \in X\}$, where X is as in Proposition 4.3. Then any pair of affine points may be mapped into $\mathcal{C}_\Pi$ by an element of $\hat{Y}$ if $p \equiv -1 \pmod 6$ and of $\hat{Y} \cup \{\hat{\tau}_{1,1}\}$ if $p \equiv 1 \pmod 6$.

Now consider the set $X_0 = \{\tau_{0,0}, \tau_{0,(p-\varepsilon)/2}, \tau_{(p+\varepsilon)/2,(p-\varepsilon)/2}, \tau_{(p-\varepsilon)/2,p-\varepsilon}\}$ of translations, where $\varepsilon \in \{-1, 1\}$ and $p \equiv \varepsilon \pmod 6$. The union $\bigcup_{\tau\in X_0} \mathcal{C}_{\Pi}\tau$ is the set of points of the affine plane. Moreover, only one element of X_0 is not in X. Let $\hat{Y}_0 = \{\hat{\tau}^{-1} \mid \tau \in X_0\}$. Then, any pair of points of Π, one an affine point and the other in $\{(0, 1, i) \mid 0 \le i \le p-1\}$, may be mapped into the set $\mathcal{C}_{\Pi}$ by an element of $\hat{Y}_0$.

The collineation σ_0 of Π moves (0, 0, 1) to the check point (0, 1, 0). Since all elements of $\hat{Y}_0$ fix each of the non-affine points, a pair of points of Π consisting of (0, 0, 1) and an affine point may be mapped into the set $\mathcal{C}_{\Pi}$ by an element of $\sigma_0\hat{Y}_0$.

Finally, we must consider pairs of non-affine points. Those which do not contain (0, 0, 1) are already in $\mathcal{C}_{\Pi}$. Pairs of the form $\{(0, 1, i), (0, 0, 1)\}$, with $i \neq 0$, may be mapped into the set $\mathcal{C}_{\Pi}$ by σ_0. For the pair $\{(0, 1, 0), (0, 0, 1)\}$, we may use the collineation σ_1.

Hence, we get a 2-PD-set $\hat{Y} \cup \hat{Y}_0 \cup \sigma_0\hat{Y}_0 \cup \{\sigma_1\}$ in the case $p \equiv -1 \pmod 6$ and $\hat{Y} \cup \hat{Y}_0 \cup \sigma_0\hat{Y}_0 \cup \{\sigma_1, \hat{\tau}_{1,1}\}$ in the case $p \equiv 1 \pmod 6$. These sets have sizes 42 and 43, respectively.

The proof for the dual code follows from the proof for C, with $\mathcal{C}_{\Pi}$ as information set: two points in the check set, $\mathcal{I}_{\Pi}$, are dealt with by ι; two affine points by $(\hat{Y} \cup \{\hat{\tau}_{1,1}\})\sigma_0$; two on $\mathcal{L}$ or $\mathcal{P}$ and one on $\mathcal{L}$ by σ_2; one in $\mathcal{A}_2$ and P by $\{\sigma_3, \hat{\tau}_{1,1}\sigma_3\}$; one affine and one on $\mathcal{L}$ by $\{\sigma_4, \sigma_4\sigma_3, \hat{\tau}_{1,1}\sigma_4, \hat{\tau}_{-1,1}\sigma_4, \hat{\tau}_{1,0}\sigma_4\}$. □

Note. The size of the set we have given in the dual case is larger than necessary as we can in fact get a set of size 41, and the actual bound is very likely lower. We include the 46-set for simplification of the argument.

We now look for specific 3-PD-sets in the affine case. For $a \in \mathbb{F}_p$ and $a \neq 0$, define collineations of $\mathrm{AG}_2(\mathbb{F}_p)$:

$$\bar{a} : (x, y) \mapsto (ax, ay), \tag{9}$$

$$\delta : (x, y) \mapsto (y, x) \tag{10}$$

for $(x, y) \in \mathrm{AG}_2(\mathbb{F}_p)$. Let $Z = \{\bar{a} \mid a \in \mathbb{F}_p^{\times}\}$ and $T = \{\tau_{a,b} \mid 0 \le a, b \le p-1\}$, the translation group of $\mathrm{AG}_2(\mathbb{F}_p)$.

Proposition 4.5. *Let $\pi = \mathrm{AG}_2(\mathbb{F}_p)$ where p is a prime, and let T be its translation group, Z and δ as defined above and in Eq. (10). For $p \ge 7$, $TZ \cup TZ\delta$ is a 3-PD-set for the code C of π using the information set of Eq. (3), and for $p \ge 5$, T is a minimal 3-PD-set for the dual code $C^{\perp}$ of π, using the information set of Eq. (4).*

Proof. First deal with the dual code: the check set is $\mathcal{C} = \{(i, j) \mid 0 \le i \le j \le p-1\}$. We may map an arbitrary triple of points in the affine plane to one of the form $(0, 0), (i_1, j_1), (i_2, j_2)$ where $0 \le i_1 \le i_2 \le p-1$ and $0 \le j_1, j_2 \le p-1$.

It is easy to translate such a triple into $\mathcal{C}$ if $i_1 = 0$ or $i_1 = i_2$ or $j_1 = 0$ or $j_2 = 0$ or $j_1 = j_2$. We will now assume that none of these equalities hold. We distinguish two cases: $j_1 < j_2$ and $j_2 < j_1$.

Case 1. $j_1 < j_2$. We can translate the triple to $(0, p-1-j_2), (i_1, p-1-j_2+j_1), (i_2, p-1)$. This triple is in $\mathcal{C}$ if $p-1-j_2+j_1 \ge i_1$.

We can also translate the triple to $(0,0)$, (i_2-i_1, j_2-j_1), $(p-i_1, p-j_1)$, which also belongs to this case. This can be translated into $\mathcal{C}$ if $p-1-(p-j_1)+(j_2-j_1) \geq i_2-i_1$. That is, $j_2-1 \geq i_2-i_1$.

If $p-1-j_2+j_1 < i_1$ and $j_2-1 < i_2-i_1$, then $p-1+j_1 < i_2$. But this is impossible, since $j_1 > 0$.

Case 2. $j_2 < j_1$. We can translate the triple to $(0, p-1-j_2)$, (i_1, j_1-j_2-1), $(i_2, p-1)$. This triple is in $\mathcal{C}$ if $-i_1+j_1-j_2 \geq 1$.

We can also translate the triple to $(0,0)$, $(i_2-i_1, p+j_2-j_1)$, $(p-i_1, p-j_1)$, which also belongs to this case. This can be translated into $\mathcal{C}$ if $-(i_2-i_1)+(p+j_2-j_1)-(p-j_1) \geq 1$. That is, $i_1-i_2+j_2 \geq 1$.

We can also translate the triple to $(0,0)$, $(p-i_2, p-j_2)$, $(p+i_1-i_2, j_1-j_2)$, which also belongs to this case. This can be translated into $\mathcal{C}$ if $-(p-i_2)+(p-j_2)-(j_1-j_2) \geq 1$. That is, $-j_1+i_2 \geq 1$.

Assuming that these three inequalities fail, we get the inequalities $-i_1+j_1-j_2 < 1$, $i_1-i_2+j_2 < 1$, $-j_1+i_2 < 1$ and, taking these in pairs, $j_1-i_2 < 2$, $-i_1+i_2-j_2 < 2$, $i_1-j_1+j_2 < 2$. Hence, $j_1-i_2 = 0$ or 1, $-i_1+i_2-j_2 = 0$ or 1 and $i_1-j_1+j_2 = 0$ or 1. Combining these equations in pairs, we see that the only possible case is that in which the three right-hand sides are all 0. This gives $i_2 = j_1$, so that $j_1 > i_1$, and $j_2 = j_1 - i_1$.

We can translate the triple $(0,0)$, (i_1, j_1), (j_1, j_1-i_1), with $i_1 < j_1$, to each of the triples to $(0, p-1-j_1)$, $(i_1, p-1)$, $(j_1, p-1-i_1)$, and $(0, i_1-1)$, $(j_1-i_1, p-1)$, $(p-i_1, p-1-j_1+i_1)$ and $(0, j_1-i_1-1)$, $(p-j_1, p-1)$, $(p-j_1+i_1, j_1-1)$. These triples are in $\mathcal{C}$ if the following inequalities hold respectively: $i_1+j_1 \leq p-1$, $2i_1-j_1 \geq 1$, and $2j_1-i_1 \geq p+1$.

Assume now that all three inequalities fail. Then $-i_1-j_1 < -p+1$, $2i_1-j_1 < 1$, and $2j_1-i_1 < p+1$. Combining these inequalities in pairs, we get the inequalities $i_1-2j_1 < -p+2$, $-2i_1+j_1 < 2$, and $i_1+j_1 < p+2$. Hence, $i_1-2j_1 = -p$ or $-p+1$, $-2i_1+j_1 = 0$ or 1, and $i_1+j_1 = p$ or $p+1$. The only case possible is when these expressions take the values $-p$, 0 and p, respectively, giving $j_1 = 2i_1$ and $3i_1 = p$. Thus $p = 3$ contrary to hypothesis.

This concludes the proof that T is a 3-PD-set for $C^{\perp}$.

To show that it is minimal, we will exhibit a triple in $\mathcal{C}$ all of whose translates by non-trivial elements of T are not in $\mathcal{C}$. In referring to translations $\tau_{i,j}$ below, we will assume that $0 \leq i, j \leq p-1$. We may write $p = 3k+1+\varepsilon$ where $\varepsilon \in \{0,1\}$. We show that the triple $(0,k)$, $(k, 3k+\varepsilon)$, $(2k+\varepsilon, 2k+\varepsilon)$ has the desired property.

The translation $\tau_{i,j}$ maps $(0,k)$ into $\mathcal{C}$ if $i \leq k$ and either $j \leq 2k+\varepsilon$ or $j > 2k+i+\varepsilon$ or if $i > k$ and $i-k \leq j \leq 2k+\varepsilon$ and not otherwise. The translation $\tau_{i,j}$ maps $(k, 3k+\varepsilon)$ into $\mathcal{C}$ if $j = 0$ or if $i \leq 2k+\varepsilon$ and $j > i+k$ or if $i > 2k+\varepsilon$ and $j > i-2k-1-\varepsilon$ and not otherwise. The translation $\tau_{i,j}$ maps $(2k+\varepsilon, 2k+\varepsilon)$ into $\mathcal{C}$ if $i \leq k$ and $i \leq j \leq k$ or if $i > k$ and either $j \leq k$ or $j \geq i$. It is a tedious, but essentially elementary, exercise to show that the only translation mapping all three points of the triple into $\mathcal{C}$ is $\tau_{0,0}$.

We give an illustration in Fig. 2, A, B and C, of the translations which move each of the points of the triple into the check set, when $p = 23$, by highlighting with heavier dots the images of the origin $(0,0)$ in these cases. The check set in this case consists of the points

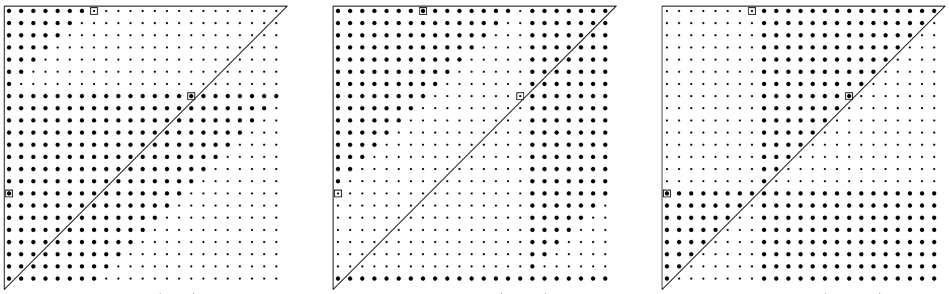


Fig. 2. Illustration of the images of the origin under translations mapping the given points into the check set for $C^\perp$ in case $p = 23$.

contained within the large triangle and the points of the triple are enclosed in small square boxes.

Now consider the code C, where the check set is $\mathcal{C} = \{(i, j) \mid p - 1 \geq i > j \geq 0\}$. We need to show that any three points can be mapped into $\mathcal{C}$ by $TZ \cup TZ\delta$. All cases in which any two of the three points are 'horizontal' or 'vertical' or lie on the line '$y = x$' can be easily translated into $\mathcal{C}$. From the first part of the proof, any remaining triple can be translated into $\{(i, j) \mid 0 \leq i \leq j \leq p - 1\}$. Moreover, unless the triple has the form $\{(i, -1), (0, j), (k, k)\}$, with i, j and k distinct, we can map it by a further translation and δ into $\mathcal{C}$. If $2i \neq -1$, we can apply the map $\bar{2}\delta$ to the triple, follow it by a suitable translation and then by δ to map the triple into $\mathcal{C}$. Finally, if $2i = -1$, we first apply the translation $(i, j) \mapsto (i, j + 1)$ and then proceed as above.

Since T is a normal subgroup of the full automorphism group of $\mathrm{AG}_2(\mathbb{F}_p)$, $TZ \cup TZ\delta$ is a 3-PD-set for C. □

Note. A similar argument yields 3-PD-sets for the projective case, for both the code and its dual. Since the arguments are so similar to those in the propositions, and since the sets obtained are not of optimal size (of the order of p^3 and p^2 respectively), we omit the result. The sets can be constructed, in a fairly obvious manner, from our results.

5. Computational results for small planes

Table 1 shows the size of some PD-sets for correcting various numbers of errors using p-ary codes of desarguesian planes of order q a power of p, and their duals, that we have obtained by computation using Magma [3] or GAP [7]. In the table, $\mathcal{D}$ denotes the design, n is the length of the code, k (respectively $k^\perp$) the dimension of C (respectively $C^\perp$), d (respectively $d^\perp$) the minimum weight, t is the number of errors corrected for a t-PD-set $\mathcal{S}$ of size $|\mathcal{S}|$, and G denotes the group spanned by $\mathcal{S}$, where T denotes the translation group (in the affine case), S a Singer group and N the normalizer of a Singer group (in the projective case), A the automorphism group, $TZ = \{\tau\bar{a} \mid \tau \in T, a \in \mathbb{F}_p^\times\}$ (see Eq. (9)), and a number in that column denotes the order of the group. The Hall and Hughes non-desarguesian projective planes of order 9 are included. Some of the computations were done using the basis of Result 2.6. Related results can be found in Limbupasiriporn [13].

Table 1
Size of t-PD-sets found by computation

		C					$C^\perp$				
$\mathcal{D}$	n	k	d	t	$\lvert\mathcal{S}\rvert$	G	$k^\perp$	$d^\perp$	t	$\lvert\mathcal{S}\rvert$	G
$AG_2(\mathbb{F}_5)$	25	15	5	2	19	T	10	10	3	25	T
									4	55	A
$AG_2(\mathbb{F}_7)$	49	28	7	2	18	T	21	14	3	49	T
				3	95	A			4	109	A
									5	227	A
									6	542	A
$AG_2(\mathbb{F}_{11})$	121	66	11	2	20	T	55	22	2	17	T
				3	119	TZ			3	121	T
				4	358	A			4	164	A
$AG_2(\mathbb{F}_{13})$	169	91	13	2	19	T	78	26	2	21	T
				3	107	TZ			3	169	T
$AG_2(\mathbb{F}_{17})$	289	153	17	3	127	TZ	136	34	3	289	T
$AG_2(\mathbb{F}_{19})$	361	190	19	3	126	TZ	171	38	3	361	T
$PG_2(\mathbb{F}_5)$	31	16	6	2	14	S	15	10	4	93	N
$PG_2(\mathbb{F}_7)$	57	29	8	2	17	A	28	14	4	158	A
				3	40	S			5	463	A
									6	949	A
$PG_2(\mathbb{F}_8)$	73	28	9	4	70	A	45	10	4	472	A
$PG_2(\mathbb{F}_9)$	91	37	10	4	109	A	54	15	5	1367	A
$PG_2(\mathbb{F}_{11})$	133	67	12	5	556	A	66	22	5	526	A
Hall_9	91	41	10	2	15	3840	54	15			
				3	47	A					
				4	123	A					
Hughes_9	91	41	10	2	21	324	54	14			
				3	82	2592					

Acknowledgements

J.D. Key thanks the Department of Mathematics at the University of Wales at Aberystwyth for their hospitality. This work was supported by the DoD Multidisciplinary University Research Initiative (MURI) program administered by the Office of Naval Research under Grant N00014-00-1-0565. EPSRC grant GR/S10193/01 support acknowledged by all the authors.

Appendix

In Tables 2 and 3 we compare the order of the automorphism group of a desarguesian projective plane of order q with the lower bound of Result 2.4 for the size of a PD-set correcting up to the full error-capability of the code. The rows up to the entry 103 are for q prime; the next, up to 4096, are for $q = 2^e$; then 3^e up to 729, 5^e up to 625, 7^e up to 343, 11^e up to 121, 13^e up to 169. The cut-off value for each of these cases indicates that for higher primes in the first, and higher prime-powers in the others, the required lower bound is greater than the group order and thus a PD-set for full error-correction cannot exist.

Table 2
Codes of desarguesian projective planes: ratio of lower bound of PD-set size to the total number of automorphisms

q	C	t	r	b	$b/\|G\|$
2	[7, 4, 3]	1	3	3	1.78571e−02
3	[13, 7, 4]	1	6	3	5.34188e−04
5	[31, 16, 6]	2	15	7	1.88172e−05
7	[57, 29, 8]	3	28	15	2.66397e−06
11	[133, 67, 12]	5	66	63	2.96572e−07
13	[183, 92, 14]	6	91	127	1.56687e−07
17	[307, 154, 18]	8	153	518	7.45302e−08
19	[381, 191, 20]	9	190	1045	6.17100e−08
23	[553, 277, 24]	11	276	4224	5.40454e−08
29	[871, 436, 30]	14	435	34336	6.87227e−08
31	[993, 497, 32]	15	496	68926	8.09014e−08
37	[1407, 704, 38]	18	703	557499	1.58839e−07
41	[1723, 862, 42]	20	861	2239792	2.80674e−07
43	[1893, 947, 44]	21	946	4493130	3.84629e−07
47	[2257, 1129, 48]	23	1128	18003387	7.56436e−07
53	[2863, 1432, 54]	26	1431	143767340	2.30999e−06
59	[3541, 1771, 60]	29	1770	1156730820	7.88031e−06
61	[3783, 1892, 62]	30	1891	2317889060	1.20941e−05
67	[4557, 2279, 68]	33	2278	18583724854	4.57754e−05
71	[5113, 2557, 72]	35	2556	74519110992	1.15422e−04
73	[5403, 2702, 74]	36	2701	149270503098	1.85129e−04
79	[6321, 3161, 80]	39	3160	1198153834565	7.89889e−04
83	[6973, 3487, 84]	41	3486	4798704980282	2.13090e−03
89	[8011, 4006, 90]	44	4005	38506833445257	9.78303e−03
97	[9507, 4754, 98]	48	4753	618058116423527	7.88682e−02
101	[10303, 5152, 102]	50	5151	2476638579630420	2.28736e−01
103	[10713, 5357, 104]	51	5356	4957694448681818	3.91402e−01
4	[21, 10, 5]	2	11	4	3.30688e−05
8	[73, 28, 9]	4	45	12	2.42677e−07
16	[273, 82, 17]	8	191	38	2.22111e−09
32	[1057, 244, 33]	16	813	180	3.27748e−11
64	[4161, 730, 65]	32	3431	1623	9.61247e−13
128	[16513, 2188, 129]	64	14325	40696	8.06865e−14
256	[65793, 6562, 257]	128	59231	3965945	2.68747e−14
512	[262657, 19684, 513]	256	242973	3625171287	8.52959e−14
1024	[1049601, 59050, 1025]	512	990551	77798319579394	6.43533e−12
2048	[4196353, 177148, 2049]	1024	4019205	206845429457074447107	6.07594e−08
4096	[16781313, 531442, 4097]	2048	16249871	75634124579444459682956291 4213	7.95531e−01
9	[91, 37, 10]	4	54	12	1.41320e−07
27	[757, 217, 28]	13	540	190	2.24564e−10
81	[6643, 1297, 82]	40	5346	17757	2.39605e−12
243	[59293, 7777, 244]	121	51516	116800246	1.92146e−12
729	[532171, 46657, 730]	364	485514	2143596829819560	4.47891e−09
25	[651, 226, 26]	12	425	364	1.19474e−09
125	[15751, 3376, 126]	62	12375	10329361	5.77697e−11
625	[391251, 50626, 626]	312	340625	28294726192048575446	3.03813e−04

Table 2 (*continued*)

q	C	t	r	b	$b/\|G\|$
49	[2451, 785, 50]	24	1666	20419	3.07341e−10
343	[117993, 21953, 344]	171	96040	6641985336739627	1.15565e−05
121	[14763, 4357, 122]	60	10406	3132513775	3.40887e−08
169	[28731, 8282, 170]	84	20449	6132177579328	4.60794e−06

Table 3
Dual codes of desarguesian projective planes: ratio of lower bound of PD-set size to the total number of automorphisms

q	C	t	r	b	$b/\|G\|$
2	[7, 3, 4]	1	4	2	1.19048e−02
3	[13, 6, 6]	2	7	4	7.12251e−04
5	[31, 15, 10]	4	16	28	7.52688e−05
7	[57, 28, 14]	6	29	122	2.16670e−05
11	[133, 66, 22]	10	67	2252	1.06013e−05
13	[183, 91, 26]	12	92	9322	1.15010e−05
17	[307, 153, 34]	16	154	160470	2.30885e−05
19	[381, 190, 38]	18	191	660742	3.90186e−05
23	[553, 276, 46]	22	277	10556212	1.35065e−04
29	[871, 435, 58]	28	436	711041773	1.42313e−03
31	[993, 496, 62]	30	497	2884912687	3.38615e−03
37	[1407, 703, 74]	36	704	189533056602	5.40004e−02
41	[1723, 861, 82]	40	862	3092795496552	3.87565e−01
4	[21, 11, 6]	2	10	7	5.78704e−05
8	[73, 45, 10]	4	28	63	1.27405e−06
16	[273, 191, 18]	8	82	23715	1.38615e−06
32	[1057, 813, 34]	16	244	25331267483	4.61238e−03
9	[91, 54, 15]	7	37	992	1.16824e−05
27	[757, 540, 38]	≥18	217	11028091675	1.30343e−02
25	[651, 425, 45]	22	226	36052751125	1.18335e−01

The columns of Table 2 are labelled as follows: q, the order of the field; C, the code; t, the error-correction capability; r, the redundancy; b, the lower bound from Result 2.4; $b/|G|$, where G is the automorphism group of the code.

Table 3 is the corresponding set for $C^{\perp}$ noting that we do not actually know the minimum weight of $C^{\perp}$ in general in the odd non-prime case, except for $q = 9$ and $q = 25$. We used the known bounds, as referenced in Section 2: see Eq. (1) and the subsequent paragraph.

References

[1] E.F. Assmus Jr., J.D. Key, Designs and their Codes, Cambridge Tracts in Mathematics, vol. 103, Cambridge University Press, Cambridge, 1992 (Second printing with corrections, 1993).

[2] A. Blokhuis, G.E. Moorhouse, Some p-ranks related to orthogonal spaces, J. Algebraic Combin. 4 (1995) 295–316.
[3] W. Bosma, J. Cannon, Handbook of Magma Functions, Department of Mathematics, University of Sydney, 1994, http://www.maths.usyd.edu.au:8000/u/magma/.
[4] N.J. Calkin, J.D. Key, M.J. de Resmini, Minimum weight and dimension formulas for some geometric codes, Des. Codes Cryptogr. 17 (1999) 105–120.
[5] K.L. Clark, J.D. Key, Geometric codes over fields of odd prime power order, Congr. Numer. 137 (1999) 177–186.
[6] K.L. Clark, J.D. Key, M.J. de Resmini, Dual codes of translation planes, European J. Combin. 23 (2002) 529–538.
[7] GAP, Groups, Algorithms and Programming, Version 4-3. The GAP Group, Lehrstuhl D für Mathematik, RWTH Aachen, Germany and School of Mathematical and Computational Sciences, University of St. Andrews, Scotland, http://www-gap.dcs.st-and.ac.uk/~gap/ 2002.
[8] D.M. Gordon, Minimal permutation sets for decoding the binary Golay codes, IEEE Trans. Inform. Theory 28 (1982) 541–543.
[9] W.C. Huffman, Codes and groups, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, vol. 2, Elsevier, Amsterdam, 1998, pp. 1345–1440 (Part 2) (Chapter 17).
[10] D.R. Hughes, F.C. Piper, Projective planes, Graduate Texts in Mathematics, vol. 6, Springer-Verlag, New York, 1973.
[11] J.D. Key, J. Moori, B.G. Rodrigues, Permutation decoding for binary codes from triangular graphs, European J. Combin. 25 (2004) 113–123.
[12] J.D. Key, P. Seneviratne, Permutation decoding of binary codes from lattice graphs, Discrete Math. (in press).
[13] J. Limbupasiriporn, Ph.D. Thesis, Clemson University, 2004.
[14] F.J. MacWilliams, Permutation decoding of systematic codes, Bell System Tech. J. 43 (1964) 485–505.
[15] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1983.
[16] G.E. Moorhouse, Bruck nets, codes, and characters of loops, Des. Codes Cryptogr. 1 (1991) 7–29.
[17] J. Schönheim, On coverings, Pacific J. Math. 14 (1964) 1405–1411.